

09/944,788

### **REMARKS**

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is obvious under the provisions of 35 U.S.C. § 103. Thus, the Applicants believe that all of these claims are in allowable form.

### **I. INFORMATION DISCLOSURE STATEMENT**

The Examiner's attention is directed to the fact that the Applicants will be filing a Supplemental Information Disclosure Statement shortly after the filing of this response. Accordingly, it is respectfully requested that the Examiner consider the references listed in the SIDS when considering this response.

### **II. REJECTION OF CLAIMS 1-6 UNDER 35 U.S.C. § 103**

Claims 1-6 stand rejected as being unpatentable over the Ericsson application (WO 00/25527, hereinafter "Ericsson") in view of the Garg et al. patent (U.S. 6,453,346, hereinafter "Garg"). The Applicants respectfully traverse the rejection.

The Examiner's attention is directed to the fact that Ericsson and Garg, singularly or in any permissible combination, fail to disclose or suggest the novel invention of identifying a set of potentially similar features shared by a new alert and one or more existing alert classes, and then updating or setting a minimum similarity requirement that must be met or exceeded by one or more features in order to identify a match between a new alert and an existing alert class, as claimed in Applicants' independent claims 1, 3, 4, 5 and 6. Specifically, Applicants' claims 1, 3, 4, 5 and 6, positively recite:

1. A method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, the method comprising the steps of:
  - (a) receiving a new alert;
  - (b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;
  - (c) updating a minimum similarity requirement for one or more features;
  - (d) updating a similarity expectation for one or more features;
  - (e) comparing the new alert with one or more alert classes, and either:
    - (f1) associating the new alert with the existing alert class that the new alert most closely matches; or
    - (f2) defining a new alert class that is associated with the new alert. (Emphasis

09/944,788

added)

3. A method for organizing alerts having a plurality of features, each feature having one or more values, the method comprising the steps of:

(a) generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding feature;

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;

(c) comparing the new alert to one or more alert classes;

(d) rejecting a match if any feature for which a minimum similarity value has been set fails to meet or exceed the minimum similarity value;

(e) adjusting the comparison by an expectation that certain feature values will or will not match, and either:

(f1) associating the new alert with the existing alert class that the new alert most closely matches; or

(f2) defining a new alert class that is associated with the new alert. (Emphasis added)

4. In an intrusion detection system that includes a plurality of sensors, each of which generates alerts when attacks or anomalous incidents are detected, a method for organizing the alerts comprising the steps of:

(a) receiving an alert;

(b) identifying a set of features that may be shared by the received alert and one or more existing alert classes;

(c) setting a minimum similarity value for one or more features or feature groups; comparing the new alert to one or more of the alert classes, and either:

(d1) defining a new alert class that is associated with the received alert if any feature or feature group that has a minimum similarity value fails to meet or exceed its minimum similarity value; or

(d2) associating the received alert with the existing alert class that the received alert most closely matches. (Emphasis added)

5. A method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, the method comprising the steps of:

(a) receiving a new alert;

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;

(c) updating a minimum similarity requirement for one or more features;

(d) comparing the new alert with one or more alert classes, and either:

(e1) associating the new alert with the existing alert class that the new alert most closely matches; or

(e2) defining a new alert class that is associated with the new alert. (Emphasis added)

09/944,788

6. A method for organizing alerts having a plurality of features, each feature having one or more values, the method comprising the steps of:

(a) generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding feature;

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;

(c) comparing the new alert to one or more alert classes;

(d) rejecting a match if any feature for which a minimum similarity value has been set fails to meet or exceed the minimum similarity value, and either:

(e1) associating the new alert with the existing alert class that the new alert most closely matches; or

(e2) defining a new alert class that is associated with the new alert. (Emphasis added)

Nowhere does Ericsson or Garg teach or even suggest the desirability of updating or setting a minimum similarity requirement for potentially similar features shared by a new alert and one or more existing alert classes. As described in the Applicants' specification (See, for example, paragraph 0063 or paragraph 0069), a minimum similarity value that sets a minimum threshold of similarity for one or more features of a new alert and corresponding features of an existing alert class may be set or updated. That is, if a feature of the new alert and the corresponding feature of the existing alert class are not close enough to at least meet the minimum similarity requirement, the new alert is not associated with the existing alert class. This eliminates the need to perform additional similarity calculations comparing the new alert and the non-matching existing alert class. The portions of Ericsson that the Examiner cites to allegedly teach this limitation in fact teach constructing a database of information (e.g., names, relations and alarm states) about network elements (e.g., devices). The network element information may be updated to reflect changes in the physical configuration "of the real network" (See, Ericsson, page 5, lines 27-28). This is not the same as updating or setting a minimum similarity requirement, e.g., for comparing features of a new alert and an existing class of alerts.

Moreover, Garg does not bridge this gap in the teachings of Ericsson. Ericsson and Garg, singularly or in any permissible combination, thus fail to teach or make obvious a method for organizing alerts into alert classes wherein a minimum similarity requirement setting a threshold for feature similarity between a new alert and one or

09/944,788

more alert classes is updated or set, as positively claimed by the Applicants in claims 1, 3, 4, 5 and 6. Therefore, the Applicants submit that independent claims 1, 3, 4, 5 and 6 fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Dependent claim 2 depends from claim 1 and recites additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 2 is not made obvious by the teachings of Ericsson in view of Garg. Therefore, the Applicants submit that dependent claim 2 also fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

### CONCLUSION


Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §103. Consequently, the Applicants believe that all of these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

10/18/04  
Date

Moser, Patterson & Sheridan, LLP  
595 Shrewsbury Avenue  
Shrewsbury, New Jersey 07702

Respectfully submitted,

  
Kin-Wah Tong, Attorney  
Reg. No. 39,400  
(732) 530-9404